REMARKS:

Applicant is in receipt of the Office Action mailed March 12, 2008. Claims 73, 75-81, 84-89, and 91-92 were pending in the application and were rejected. Claims 73, 78, 84, 88 and 89 have been amended. Claims 75-76, 81, 85-87, and 91 have been canceled. New claims 93-96 have been added. Claims 73, 77-80, 84, 88-89, and 92-96 are now pending in the application. Reconsideration of the case is earnestly requested in light of the following remarks. Applicant notes that the following remarks extrapolate on points raised in the undersigned's telephone conference with the Examiner held on July 9, 2008.

Section 103 Rejection

Claims 73, 75-81, 84-89, 91 and 92 were rejected under 35 U.S.C. 103(a) as being unpatentable over Obenhuber et al., U.S. Patent No. 6,144,638 (hereinafter "Obenhufer") in view of Subramaniam et al., U.S. Patent No. 6,640,302 (hereinafter "Subramaniam"), and further in view of Farah ("Encrypted Hypertext Transfer Protocol –UGGC/1.0", April, 2000, Network Working Group) (hereinafter "Farah"). Applicant respectfully traverses this rejection.

Claim 73 recites in pertinent part:

> … wherein said decrypted data includes a request for a web page in a second Internet domain that is different from the first Internet domain, wherein said request is directed to a first address hosted by the first server in the first Internet domain by directing the request to a URL including an encrypted address of said web page appended after an unencrypted form of the first address;
>
> said first server decrypting the encrypted address of the web page;
>
> in response to said decrypting, said first server communicating with a second server in the second Internet domain to retrieve the web page from the second Internet domain;

Applicant respectfully submits that the combination of cited references does not teach these limitations in combination with the other limitations recited in claim 73.

First, the references do not teach directing a request for a web page in a second Internet domain to a first address hosted by the first server in the first Internet domain by directing the request to a URL including an encrypted address of the web page appended after an unencrypted form of the first address.

The Office Action relies on Farah to teach the recited limitation regarding the URL including the encrypted address of the web page. However, the combination of Farah with the other cited references does not teach a URL such as recited in claim 73. In Section 2.2 Farah teaches as follows (emphasis added):

"URLs <u>**MUST**</u> be encrypted in one of the following ways:

1) total encryption: **the entire URL is encrypted**. …

2) partial encryption: there are two acceptable syntaxes:
- the <u>**host part**</u> of the URL is encrypted, the rest is not. …
- the <u>**host part**</u> is encrypted, and so is the abs_path…

In both cases the entire host part <u>**MUST**</u> be encrypted. …

3) null encryption: **the entire URL is NOT encrypted**. …"

Thus, Farah's URL encryption scheme requires that the <u>host part</u> of the URL <u>must</u> be <u>**encrypted**</u> (unless null encryption is used, in which case none of the URL is encrypted). <u>**In sharp contrast, in the URL recited in claim 73, the host part of the URL specified by the first address (i.e., the first address to which the request is directed) is unencrypted**</u>. Therefore, Farah's encryption technique cannot be used to produce a URL such as recited in claim 73 since Farah's system <u>**requires**</u> the host part of the URL to be encrypted, whereas the host part of the URL in claim 73 is unencrypted.

<u>**Second,**</u> the combination of references also fails to teach the recited limitations of the "first server decrypting the encrypted address of the web page, and in response to said decrypting, the first server communicating with a second server in the second Internet domain to retrieve the web page from the second Internet domain."

As recited in claim 73, the request is directed to the first address hosted by the first server in the first Internet domain by directing the request to a URL that includes an unencrypted form of the first address in the first Internet domain. The URL also includes an encrypted address of the web page in the second Internet domain appended after the unencrypted form of the first address. The first server decrypts the encrypted address of the web page and then communicates with the second server in the second Internet domain to retrieve the web page from the second Internet domain.

The Office Action relies on Subramaniam to teach the recited limitation regarding the encrypted address of the web page being appended after the unencrypted form of the first address in the URL. In particular, the Office Action cites Subramaniam's teaching at Col. 7. However, Subramaniam here teaches the server appending one URL to another for the purpose of returning the aggregate URL to the client from which the request was originally received. The web browser on the client then performs a redirect using the aggregate URL returned by the server. Thus, the client performs a first request to a first server. The first server then returns a URL to the client, and the client then performs a second request to a second server specified by the URL.

In contrast, in claim 73, the first server decrypts the encrypted address of the web page and then communicates with the second server in the second Internet domain to retrieve the web page from the second Internet domain and return the web page to the client. This subject matter is not taught by the cited references, taken either singly or in combination.

Third, Applicant notes that the combination of references cited in the Office Action does not solve the problem which is solved by the invention claimed in claim 73. Suppose for example, that a user desires to access a web page hosted on a server in an Internet domain "xyz123456.com". For example, suppose that the user desires to access a web page specified by the address "xyz123456.com/directory1/page1.html". Suppose still further that the user does not want any intermediate snooper that might be between the user's client computer and the server at xyz123456.com to be able to determine that the user is accessing the xyz123456.com Internet domain.

In this example, the "xyz123456.com" Internet domain corresponds to the "second Internet domain" recited in claim 73, and the address "xyz123456.com/directory1/page1.html" corresponds to the recited address of the web page in the second Internet domain. As recited in claim 73, the request is directed to a first address hosted by a first server in a first Internet domain, e.g., where the first server provides an anonymization service as described in the present specification. Thus, the web page address "xyz123456.com/directory1/page1.html" may be encrypted and included in a URL such that the encrypted address of the web page is appended after an unencrypted form of the first address hosted by the first server in the first Internet domain. In response to receiving the request, the first server may decrypt the encrypted address of the web page and then communicate with a server in the "xyz123456.com" Internet domain to retrieve the requested web page and then return the web page to the user.

Thus, the problem described above is solved because: 1) The address of the requested web page is encrypted; and 2) The request is sent to the first Internet domain, i.e., an Internet domain other than the second Internet domain where the requested web page is hosted (e.g., other than the "xyz123456.com" domain in this example). Thus, not only does the invention prevent intermediate snoopers from knowing the address of the web page being requested, but it also prevents them from even knowing which Internet domain hosts the requested web page (since the request is not sent to the Internet domain that hosts the requested web page).

The references cited in the Office Action do not solve these problems. The Obenhufer reference relates generally to a system for providing users with access to a network such as the Internet. Obenhufer teaches a multi-tenant unit that includes an encryption/decryption engine. The encryption/decryption engine encrypts each outgoing data packet and decrypts each incoming data packet. (Col. 4, lines 1-35). Thus, Obenhufer's encryption/decryption engine simply encrypts and decrypts the data exiting and entering the multi-tenant unit. However, Obenhufer does not solve the problem discussed above. For example, although the data packets are encrypted, an intermediate snooper would still know which server the data packets are being directed to.

The Subramaniam reference relates generally to a system which allows secure external access to a secure network. Thus, Subramaniam generally pertains to a method for providing secure access to a secure network, but is not concerned with the problem of providing anonymization for a user of a client computer, such as described above.

The only reference that directly pertains to the problem of protecting a user from snoopers that attempt to determine what the user is trying to access is Farah. However, Farah, taken either singly or in combination with the other references, does not fully solve the problem discussed above. Farah teaches that the URL of the web page being requested may be totally or partially encrypted. However, the web page request is still sent to the server that hosts the web page. For example, in the above example, even though a snooper may not be able to determine the exact web page that the user is trying to access, the snooper can still determine that the user is accessing the "xyz123456.com" Internet domain because the TCP/IP packets are sent to the server in the "xyz123456.com" Internet domain. Thus, the snooper can simply inspect the

TCP/IP packets to determine the IP address to which they are being sent and can then determine which Internet domain contains this IP address. Thus, the problem of anonymization as discussed above is not solved by Farah, taken either singly or in combination with the other cited references.

Applicant thus respectfully submits that claim 73 is patentably distinct over the cited references for at least the reasons set forth above. Inasmuch as the other independent claims 84, 89, and 94 recite similar limitations as those of claim 73 discussed above, Applicant respectfully submits that these claims are also patentably distinct over the cited references. Applicant notes that claim 94 is directed to an alternative embodiment and recites the further limitation of the first server receiving the encrypted data originating from the computer behind the firewall via a second server in a second Internet domain. (The "third Internet domain" in claim 94 corresponds to the "second Internet domain" in claim 73—that is, the requested web page in claim 94 is in a third Internet domain, as opposed to a second Internet domain as in claim 73.)

Since the independent claims have been shown to be patentably distinct, Applicant respectfully submits that the dependent claims are also patentably distinct, for at least this reason. Applicant also respectfully submits that the dependent claims recite further distinctions over the cited art. For example, amended claim 78 recites the further limitations of:

> wherein said retrieved web page includes one or more links pointing to the second Internet domain, wherein the method further comprises:
>
> before sending the encrypted data including the retrieved web page to the computer, the first server modifying the retrieved web page by modifying the one or more links to point to the first Internet domain instead of the second Internet domain.

Applicant respectfully submits that the cited references, taken either singly or in combination, do not teach these limitations in combination with the other limitations recited in claim 73. Applicant thus submits that claim 78, and claims 88, 93, and 96 which recite similar limitations, are separately patentable over the cited references.

CONCLUSION:

Applicants submit the application is in condition for allowance, and an early notice to that effect is requested.

Applicant has petitioned herewith for what is believed to be the appropriate extension of time. If any further extensions are necessary to prevent the above-referenced application from becoming abandoned, Applicant hereby petitions for such extension.

The Commissioner is authorized to charge any fees that may be required, or credit any overpayment, to Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C. Deposit Account No. 501505/6002-03300/DMM.

Respectfully submitted,

Date: July 14, 2008

By: /Dean M. Munyon/
Dean M. Munyon
Reg. No. 42,914

Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P. O. Box 398
Austin, Texas 78767
(512) 853-8847